Vibration-based Key Exchange between Two Smart Devices on the Desk

Alisa Arno†, Kentaroh Toyoda†, Yuji Watanabe††and Iwao Sasase†
†Dept. of Information and Computer Science, Keio University
3-14-1 Hiyoshi, Kohoku, Yokohama, Kanagawa 223-8522, Japan,
Email: {arno, toyoda}@sasase.ics.keio.ac.jp,sasase@ics.keio.ac.jp
††IBM Research - Tokyo, IBM Japan Ltd.
19-21 Nihonbanshi, Hakozaki-cho, Chuo-ku, Tokyo 103-8510, Japan.
Email: muew@jp.ibm.com

***Abstract*—The man-in-the-middle attack is a real concern in mobile NFC (Near Filed Communication) payment and data sharing applications. Hence, it is necessary to exchange a secret key between devices without wireless communication. In this paper, we propose a non-interactive vibration-based key exchange between two smart devices on the desk. In our scheme, two devices are assumed to be placed next to each other. Each device then vibrates with patterns converted from a key to be exchanged and measures them with accelerometers. Finally, each key is recovered from measured acceleration. We implement our scheme with Android smartphones to show the effectiveness of the proposed scheme.**

I. Introduction

Due to the popularization of smartphones and tablets, electronic payment services and data sharing applications using NFC (Near Field Communication) are expanding. However, NFC is vulnerable to the man-in-the-middle in which an attacker existing between devices eavesdrops or tampers information [1]. This attack is called the man-in-the-middle attack. To prevent the man-in-the-middle attack, S. Drimer et al. proposed an authentication scheme which checks devices' physical proximity [2]. They proposed a distance bounding protocol which tests a physical distance between devices by measuring devices' communication delay. This proposal is pointed out to be easily affected by the communication delay [2].

Recently, smartphones' sensor modules, e.g., GPS, accelerometer, microphone and light sensor, are used to prevent the man-in-the-middle attack. Many sensor-based authentication schemes have been proposed in industry and academia [3]–[15]. Many sensor data can be used for it: (i) temperature [6], [7], (ii) acceleration [10], [13]–[15], (iii) location information [5], [11], (iv) RF (Radio Frequency) signals [8], [11], [12], (v) audio [3], [4], [9], [11], (vi) light [3], [4], [9], (vii) exhaust gas [7], (viii) humidity [7], and (ix) altitude [7]. In these proposals, it is important to use information that (i) two legitimate devices can measure the same information and (ii) a device which is not in the proximity should guess the measures data. However, these schemes, e.g., [10], [14] have to be attached physically, and the acceleration information might be predicted by observing users' movement by an attacker. Hence, it is necessary to propose a key exchange scheme without leaking motion of smart devices.

In this paper, we propose a vibration-based key exchange between two smart devices on the desk. An exchanged key is converted into vibration patterns and both devices measure their acceleration information. Our proposal does not need user's special operation to safely exchange keys between communication devices. We implement our scheme with Android smartphones and evaluate the efficiency by actually measuring acceleration of the vibration.

The rest of this paper is constructed as follows: we summarize related work in Section II. The proposed scheme is described in Section III. Evaluation is shown in Section IV. We conclude our discussion in Section V.

II. Related Work

Recently, many works have been proposed that use sensor information as key exchange and proximity-based authentication of two devices, e.g., [3]–[15]. T. Halevi et al. proposed a secure proximity detection scheme for a NFC enabled mobile payment system [3], [4]. In these schemes, audio and light measured with smartphones are used as location information in order for the authority to check whether a device is truly used for payment. D. Ma et al. proposed a geographical authentication scheme using GPS or WiFi-based positioning system [5]. In this proposal, a device verifies the proximity of a communicating device with GPS information. P. Urien et al. proposed the identity-based authentication for RFID (Radio Frequency IDentification) with the temperature of surroundings by the reader and the tag [6]. M. Miettinen et al. proposed a paring scheme for wearable devices with audio and light information [9]. B. Shrestha et al. proposed to use four sensor modalities, which are ambient temperature, exhaust gas, humidity, and altitude for proximity test [7]. Y. Shu et al. proposed an access control system with acceleration information [13]. H. Truong et al. examined which sensory information is useful for paring among GPS, WiFi, Bluetooth, and audio information [11]. S. Mathur et al. proposed to utilize the fact that if two devices are sufficiently close, they receive almost the same RF sources, i.e., FM or TV signals and use this information for proximity test [8]. T. Wang et al. use

RSS (Received Signal Strength) of the physical-layer for far proximity verification [12].

However, it is difficult to control the valid range of two devices. For example, when light or audio information are used for authentication in in-door situations, an attacker who is in the same room, might be authenticated since he/she can obtain valid information. Therefore, schemes using light information or the strength of a radio wave of Wi-Fi are suitable for an authentication for several smart devices which are placed in the same place, e.g., the same room or floor. On the other hand, they are not appropriate for an authentication for payment. Recently, methods for determining whether two smart devices are in close proximity, say within 1 cm, have been proposed. R. Mayrhofer et al. proposed a secure pairing with accelerometer [10]. In this scheme, two devices are put together back-to-back by a user. They are then shaken to sense the same acceleration. M. Mehrnezhad et al. proposed a NFC payment system preventing man-in-the-middle attacks by using acceleration [14]. A user bumps his/her smartphone to a register, and both the smartphone and register measure acceleration. If measured values are similar, the smartphone is authenticated for payment. W. Gu et al. proposed an authentication scheme between two smartphones using vibration [15].

However, these schemes, e.g., [10], [14], have to be attached physically, and the acceleration information might be predicted by observing users' movement by an attacker. Hence, it is necessary to propose a key exchange scheme without leaking motion of smart devices.

III. Proposed Scheme

Here, we propose a non-interactive vibration-based key exchange between two smart devices on the desk. In this proposal, two devices are assumed to be placed next to each other on the desk. Each device then vibrates with patterns converted from a key to be exchanged and measures them with accelerometers. Finally, each key is recovered from measured acceleration, and keys will be used for encrypting a message. The reason why we choose vibration as a communication medium is that a wave can only propagate on a general desk and its communication range is very narrow. As we will show later, even if an attacker's device eavesdrops 1cm away from legitimate devices, the secret key cannot be recovered. In addition, it is impossible for an attacker to find out vibration patterns visually. In the following, we first describe the system model and then the detailed algorithm.

A. System Model

The proposed key exchange scheme requires three entities: two smart devices, e.g., a smartphone, tablet cash register, and a desk. We also assume that two smart devices are equipped with a near field wireless communication module e.g., Bluetooth LE (Low Energy), an accelerometer module and a microprocessor to process measurement data. Note that wireless communication modules are required to transfer data encrypted with an exchanged key because it is too slow to send entire data with vibration. We assume that two smart devices, d_1 and d_2, are on the table next to each other, and device d_1 wants to send data to device d_2.

B. Algorithm

Fig. 1 shows the flowchart of our proposal scheme. Two devices, which are denoted as d_1 and d_2, exchange their own keys with vibration. First, device d_1 sends a key exchange request to device d_2.

Then, device d_1 and d_2 convert their own secret keys k_1 and k_2 into vibration patterns. For example, device d_1 made k_1 as (0, 1, 1, 0, 0, ...). At 0 bit, device d_1 will not vibrate, and at 1 bit, device d_1 will vibrate. Fig. 2 shows an example of converting a secret key to a vibration pattern. After k_1 and k_2 convert to vibration patterns, device d_1 and d_2 vibrate following vibration patterns and measure acceleration information. Each acceleration is measured by the accelerometer of devices.

Let $A_j = \{(a_{x,j,1}, a_{y,j,1}, a_{z,j,1}), \cdots, (a_{x,j,T}, a_{y,j,T}, a_{z,j,T})\}$ denote device d_j (j = 1 or 2) 's three-axes acceleration from time 1 to T. Because of the high sensitivity of the device's accelerometer A_j can be easily affected by even just a little amount of vibration. Hence, noise is eliminated by using (1)-(3) that are shown in [16]. We present $A'_{x,j,t}$, $A'_{y,j,t}$ and $A'_{z,j,t}$ indicates the acceleration after noise is removed.

$$A'_{x,j,t} = \frac{-3a_{x,j,t-1} + 2a_{x,j,t} + a_{x,j,t+1}}{4}, \tag{1}$$

$$A'_{y,j,t} = \frac{-3a_{y,j,t-1} + 2a_{y,j,t} + a_{y,j,t+1}}{4}, \tag{2}$$

$$A'_{z,j,t} = \frac{-3a_{z,j,t-1} + 2a_{z,j,t} + a_{z,j,t+1}}{4}, \tag{3}$$

In order to get high accuracy, the strength of acceleration is calculated with three-axis measurements $A'_{x,j,t}, A'_{y,j,t}, A'_{z,j,t}$ as represented in (4).

$$R_{j,t} = \sqrt{A'^2_{x,j,t} + A'^2_{y,j,t} + A'^2_{z,j,t}}, \tag{4}$$

After the measurement, a key is recovered with the acceleration information. Since R_j involves the violation made by its own device, which we denote as I_j, it is required to eliminate this component.

$$R'_{j,t} = \begin{cases} R_{j,t} - I_{j,t} & (R_{j,t} > I_{j,t}) \\ 0 & (otherwise). \end{cases} \tag{5}$$

Although the device cannot measure both R_j and I_j at the same time, each device knows the vibration pattern which they are about to perform. Therefore, it is possible to predict I_j. Finally, binary data is recovered from R'_j by setting a threshold m_j. From a preliminary experiment, we set the threshold m_j as a average of acceleration R'_j. The reason we use the average of the acceleration is we can get the highest similarity. k_j will be recovered as (6).

$$k'_{j,t} = \begin{cases} 1 & (R'_{j,t} > m_j) \\ 0 & (otherwise) \end{cases} \tag{6}$$

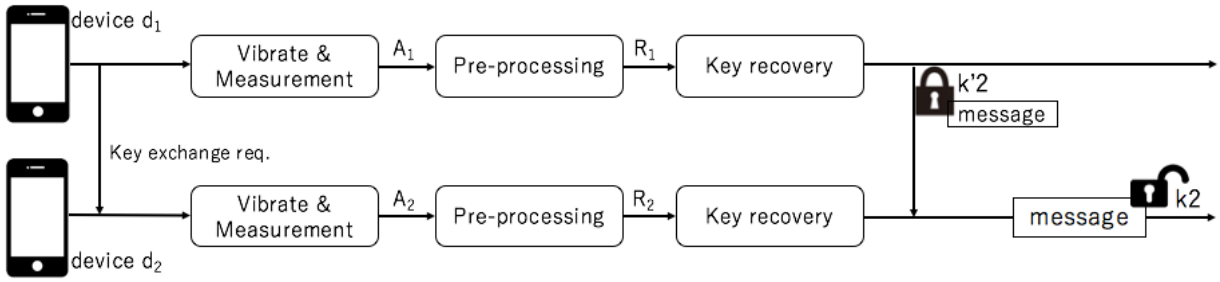


Fig. 1: Flowchart of the proposed scheme.

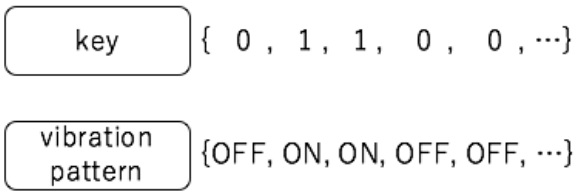


Fig. 2: Convert k_1 to a vibration pattern.

Fig. 3: Experiment environment.

After k_j is recovered, device d_1 uses key k'_2 to encrypt a message to send to device d_2. Device d_2 will decrypt the massage by k_2. Similarly, on device d_2 side, key k'_1 will be used to encrypt a message to device d_1, and d_1 decrypts this encrypted message using k_1.

C. Discussion

The advantage of our scheme is as follows. The first one is that our scheme generates a one-time authentication code because the vibration pattern can be changed every time. The second one is that our scheme can operate everywhere as long as there is a desk. The third one is that even if an attacker exists in the vicinity of devices, he/she cannot observe each vibration pattern which two smart devices make. In addition, our scheme does not require time synchronization between two smart devices because they start vibrating and measuring just after receiving a measurement request message.

IV. Evaluation

We evaluate the efficiency of our scheme with Android phones Nexus 5 in the real environment. Since we do not have a tablet cash register with a vibration function, we used two Nexus 5s as a smart phone and a tablet cash register. Both devices d_1 and d_2 randomly generate secret keys k_1 and k_2, and convert them into vibration patterns and let both devices vibrate. We first show whether the same acceleration information can be observed in two smart devices when they vibrate at the same time. We then compare the real acceleration R_j with the expected acceleration I_j. We will show that the similarity of the binary data from expected acceleration and the binary data from the vibration pattern. The similarity sim is represented as Eq. (7).

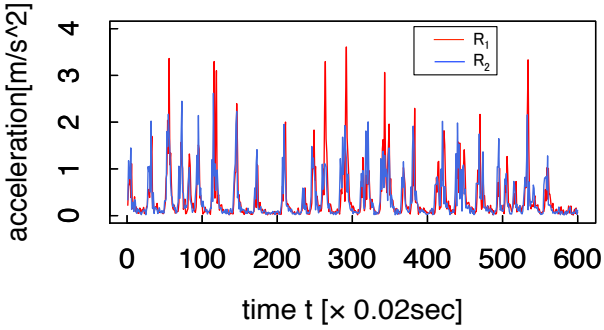


Fig. 4: Acceleration measured in two smart devices.

$$sim = \frac{k_{j,t} \wedge k'_{j,t}}{T} \times 100[\%] \tag{7}$$

Finally, we also evaluate how much similarity sim is achieved by an attacker which is placed 1 cm away from two smart devices and measures their acceleration at the same time.

Fig. 3 shows how two Nexus 5s are placed next to each other on the desk. In order to calculate sim, we repeatedly measured acceleration as many as 20 times for each metric. The vibration interval between any adjacent bit is 0.2 sec. We fix the sampling interval as 0.02 sec since we have confirmed that it is enough to observe the movement. Since the accelerometer is highly sensitive to vibration, it will be influenced by noise if the sampling interval is too short. We also set $I_{t,j} = 5[m/s^2]$.

A. Acceleration of two smart devices vibrating at the same time

Fig. 4 shows the measured acceleration of two smart devices vibrating at the same time. In this figure, the red and blue lines

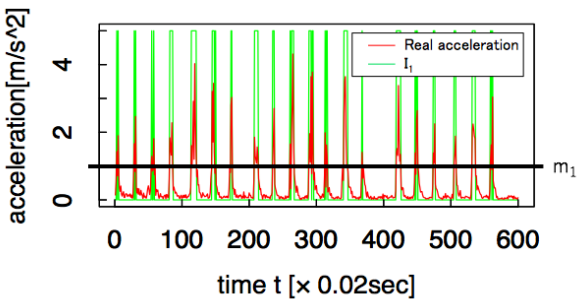
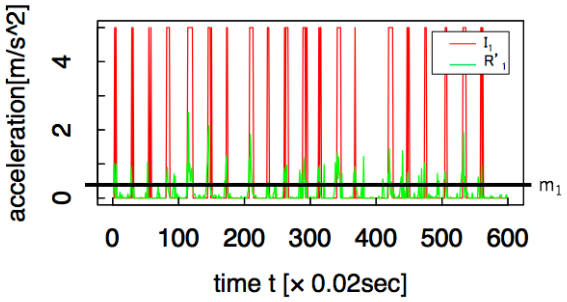
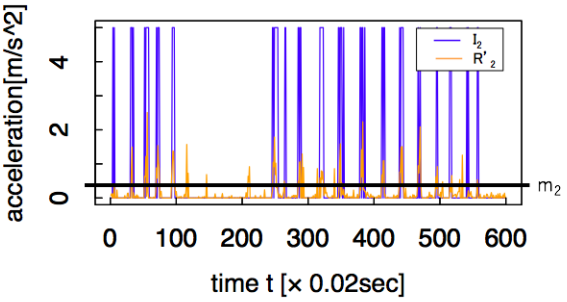


Fig. 5: Comparing actual acceleration measured by a device with expected acceleration I_j.



(a) Acceleration measured at device d_1.



(b) Acceleration measured at device d_2.

Fig. 6: Comparison between expected acceleration and actual acceleration in two smart devices.

show acceleration measured by device d_1 and d_2, respectively. Ideally, these lines should be the same in terms of the timing of spikes and magnitude of acceleration. From Fig. 4, on the one hand, most of the spikes are simultaneously observed at smart devices. On the other hand, magnitude of acceleration sometimes differs in two devices, e.g., $t = 50, 260, 340$. However, this proble might be not so serious since we set a threshold m_j for deciding $k'_{j,t} = \{0, 1\}$.

B. Converting a secret key into a vibration pattern

We then show whether the setting of m_j is appropriate. Again, m_j is calculated by the average of magnitude of measured acceleration. Fig. 5 shows the time series of measured acceleration, m_1 and I_1 when only device d_1 is vibrated. As

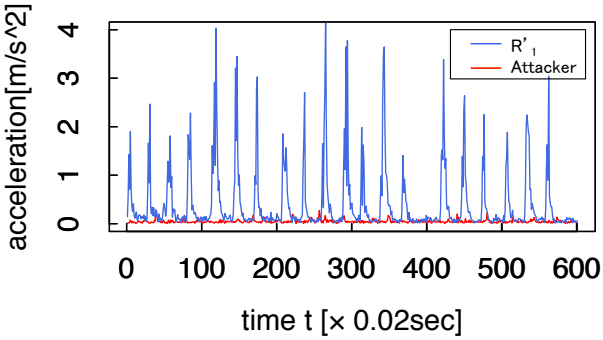


Fig. 7: Magnitude of acceleration measured by an attacker and the closer legitimate device.

we can see from this figure, any key element $k_{1,t} = 1$ is successfully decoded as '1' in this measurement.

C. The similarity of the binary data from expected acceleration and vibration patterns

Fig. 6 shows comparison between expected acceleration and actual acceleration in two smart devices calculated from (6). In Fig. 6(a), the red and green lines show I_1 and R'_1, respectively. Similarly, the blue and orange lines show I_2 and R'_2, respectively. Although, the magnitude of I_j and R'_j are different, we can change R'_j into k'_j by using m_j accurately.

From (7), the similarity between k_1 and k'_1 is 83.3%, and the similarity between k_2 and k'_2 is 85.8%. Although device d_j cannot decrypt a message only when $sim = 100\%$, if we use an error correction scheme, e.g., Reed-Solomon error correction coding, the similarity gets as close as 100%. However, it will need more time to exchange a key.

D. Performance of An Attacker

Fig. 7 shows the comparison of acceleration measured by the attacker and device d_1. In Fig. 7, the red and blue lines show acceleration measured by an attacker and R'_1, respectively. As can be seen from this result, an attacker is not able to sense vibration to recover a key even if his/her device is placed 1 cm away from a legitimate device. We also measure the similarity between attacker's and device d_1's acceleration and it results in 53.6%. This means that the attacker's success probability is almost the same as random guessing, i.e., $sim = 50\%$. From this result, we can say that an attacker cannot eavesdrop the key even if an attacker's device is placed in the vicinity of legitimate devices.

V. Conclusion

We have proposed a non-interactive vibration-based key exchange between two smart devices on the desk. In our proposal, vibration and acceleration are used as communication medium for two devices to exchange secret keys. Since there is no need to use radio communication, our proposal can prevent the man-in-the-middle attack.

Our method assumes that two smart devices are on the desk. From the evaluation, it is shown that the similarity between

k_1 and k_1' is 83.3%, and the similarity between k_2 and k_2' is 85.8%. The similarity between an attacker's and device d_1's acceleration is 53.6%. From this result, we can say that an attacker cannot eavesdrop the key even if the attacker's device is placed in the vicinity of legitimate devices.

For the future work, it is necessary to consider a faster and more accurate scheme. We should also consider the case where an attacker physically exists between two smart devices, and a key exchange scheme within more than three smart devices.

ACKNOWLEDGMENT

This work is partly supported by the Grant in Aid for Scientific Research (No.26420369) from Ministry of Education, Sport, Science and Technology, Japan.

REFERENCES

[1] K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones," *Radio Frequency Identification System Security: RFIDsec*, vol. 12, p. 21, 2012.

[2] S. Drimer, S. J. Murdoch *et al.*, "Keep your enemies close: Distance bounding against smartcard relay attacks." in *USENIX Security*, vol. 2007, 2007.

[3] T. Halevi, D. Ma, N. Saxena, and T. Xiang, "Secure proximity detection for nfc devices based on ambient sensor data," in *ESORICS*. Springer, 2012, pp. 379–396.

[4] T. Halevi, H. Li, D. Ma, N. Saxena, J. Voris, and T. Xiang, "Context-aware defenses to rfid unauthorized reading and relay attacks," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 307–318, 2013.

[5] D. Ma, N. Saxena, T. Xiang, and Y. Zhu, "Location-aware and safer cards: enhancing rfid security and privacy via location sensing," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 2, pp. 57–69, 2013.

[6] P. Urien and S. Piramuthu, "Identity-based authentication to address relay attacks in temperature sensor-enabled smartcards," in *European Conference on Smart Objects, Systems and Technologies (SmartSys-Tech)*. VDE, 2013, pp. 1–7.

[7] B. Shrestha, N. Saxena, H. T. T. Truong, and N. Asokan, "Drone to the rescue: Relay-resilient authentication using ambient multi-sensing," in *Financial Cryptography and Data Security*. Springer, 2014, pp. 349–364.

[8] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2011, pp. 211–224.

[9] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, "Context-based zero-interaction pairing and key evolution for advanced personal devices," in *ACM Conference on Computer and Communications Security (CCS)*, 2014, pp. 880–891.

[10] R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Transactions on Mobile Computing*, vol. 8, no. 6, pp. 792–806, 2009.

[11] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication," in *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2014, pp. 163–171.

[12] T. Wang, Y. Liu, and J. Ligatti, "Fingerprinting far proximity from radio emissions," in *ESORICS*. Springer, 2014, pp. 508–525.

[13] Y. Shu, Y. J. Gu, and J. Chen, "Dynamic authentication with sensory information for the access control systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 427–436, 2014.

[14] M. Mehrnezhad, F. Hao, and S. F. Shahandashti, *Tap-Tap and Pay (TTP): Preventing Man-In-The-Middle Attacks in NFC Payment Using Mobile Sensors*, 2014.

[15] W. Gu, Z. Yang, L. Shangguan, X. Ji, and Y. Zhao, "Toauth: Towards automatic near field authentication for smartphones," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2014, pp. 229–236.

[16] E. J. Keogh and M. J. Pazzani, "Derivative dynamic time warping." in *Sdm*, vol. 1. SIAM, 2001, pp. 5–7.